

COUNTY OF LOS ANGELES CHIEF INFORMATION OFFICE

500 West Temple Street 493 Kenneth Hahn Hall of Administration Los Angeles, CA 90012

> Telephone: (213) 974-2008 Facsimile: (213) 633-4733

June 14, 2007

To:

Supervisor Zev Yaroslavsky, Chairman

Supervisor Gloria Molina Supervisor Yvonne B. Burke

Supervisor Don Knabe

Supervisor Michael D. Antonovich

From:

Jon W. Fullinwider

Chief Information Officer

Subject:

FISCAL YEAR 2007-08 BUSINESS AUTOMATION PLAN SECURITY

SURVEY

Attached is an assessment of the Fiscal Year 2007-08 Business Automaton Plan (BAP) Security Survey that is completed annually by each department. The information compiled was based on departmental responses to survey questions and used to develop a security effectiveness rating for each department. While many factors were assessed, the last row in the attached matrix reflects the overall assessment by department of compliance with Board adopted security policies and standards.

The majority of departments were rated with some deficiencies (yellow) while 11 departments were rated good (green). Five departments were noted with major deficiencies (red) for various reasons such as security updates not being current or failure to require Acceptable Use Agreements (Board Policy 6.101) to be signed as a condition to use County systems. Departments that have obsolete operating systems were noted as deficient because those systems cannot be updated with current security software that would protect them from viruses. The inability to maintain current security software levels can lead to enterprise-wide security events affecting the County's ability to provide public services.

Each Supervisor June 14, 2007 Page 2

Since the Security Survey is part of the annual BAP process and is a self assessment of compliance, my Office has engaged the Institute for Critical Information Infrastructure Protection that is part of the University of Southern California, Marshall School of Business to conduct four independent security reviews per quarter of selected County departments. The purpose of the reviews is to independently validate the responses provided in the annual Security Survey. The results of the reviews will validate compliance and identify areas requiring improvement to assist departments in strengthening their information security programs.

Security Reviews are scheduled to begin in July 2007 and will continue over the course of the calendar year. All findings will be provided to the affected departments as well as the Chief Executive Officer, Auditor-Controller, and your Board. Departments will be expected to develop corrective action plans to remediate all areas of weakness noted.

If you have any questions, please contact me or Al Brusewitz, Associate CIO, at (562) 940-3873 or e-mail to abrusewitz@cio.lacounty.gov.

JWF:AB:ygd

Attachment

c: Department Heads Department CIOs

P:\Final Documents\CIO\CIO Memo-2007 Security Survey 6-7-07 (2) (2) (3).doc

Question	Affrm Act	AWM	APD	Ann Cut	Acceent	ζ.	0	C C
Compliant with Board security policies	°N	No No	Yes	N	Voc	3		SOO X
If not, do you have a compliance plan	Voe	Voc	NILA		37.4	165	ONI	Yes
Will you be compliant in 2007/2008	201	700	W.A.	ien.	N/A	N/A	Yes	N/A
Decident of the second of the	x es	Yes	N/A	Nove	N/A	N/A	Yes	N/A
Manual ISCO	Full fime	Part time	Full time	Full time	Part time	Part time	Part time	Part Time
Attend 1950 regularly	S N	Yes	səA	90	Yes	Yes	cN	Yes
SET TOTAL	Yes	Yes	Se),	8	Yes	Yes	SZ	Yes
oer participation	No	Yes	sə _k -	SN.	Yes	Yes	N	Voc
Have a department computer emergency resp. (DCERT)	No	Yes	Хes	S/	Хes	2	2 2	Vec.
Systems implemented and configured to security standards	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Dasswords observed acceptable use agreement	Yes	Yes	Yes	I ON	Yes	Yes	Yes	Yes
Dhysical sociality massing in all	Yes	Yes	Yes	No	SeX	Yes	Yes	Yes
Data capitization with the discention	Yes	Yes	/ Yes	February S	SeX	Yes	Yes	Yes
Formal sociality development life	Yes	Yes	Yes	Yes	SeX	Yes	Yes	Yes
Vilhamahiliti accounty development mecycle	8	2	Yes	No	Хes	2	8	Yes
Pomoto cocce to the scanning performed	S	No	No	No	No	Yes	SZ.	Ves
Two Eactor authorities	Yes	No	No	Yes	Yes	Yes	Yes	Yes
Remote dial access allowed	Xex.	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Have identified encoding to the control of the cont	o Z	<u>.</u>	N/A	No	No	oN.	ΝΘ	No
Require remote access software	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Do voli have obsolete committee constitution	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Do voli have a fechnology refresh alon	ON ;	o N	No	Yes	No	Yes	ON	No
Do vou rerailire firewalls on destrons and lastons	Yes	Yes	Yes	Non	Yes	Yes	Yes	Yes
Host intrusion on servers	0 2	Yes	Yes	No	Yes	Yes	Yes	Yes
le antivirue coftware inctalled and consent	9N	2	So	No	Yes	Yes	8	S _N
le aptivitie software installed and current	Yes	Yes	Yes	WIGH		Yes	Yes	Yes
le natch management software utilities	Yes	Yes	Yes	J. D.W.	, Yes	Yes	Yes	Yes
Are security software natches current	Yes	No	Yes	No	Yes	Yes	Yes	Yes
RCP Plan	Yes	NO NO	Yes	Maria	Yes	Yes	Yes	Yes
Origin Mamt Dlan	Kes	Yes	Yes	No	Yes	Yes	Yes	Yes
Crais inglint rial	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes

Color Codes
Good Security Program
Some Deficiencies
Major Weaknesses
Not Applicable

Departmental Security Rating

Question	CAO	CIO	CSSD	DCFS	Com Dev	883	Consumar	3000
Compliant with Board security policies	Yes	Yes	Yes	S _N	Yes	Yes	Yes	Vec
If not, do you have a compliance plan	N/A	N/A	N/A	Yes	N/A	N/A	ν/IN	N/A
Will you be compliant in 2007/2008	N/A	N/A	N/A	Yes	A/N	N/A	V/V	V/IV
Designated security officer	Part Time	Full Time	Part Time	Part Time	L _C	Part Time	Part Time	Dart Time
Attend ISSC regularly	No	Yes	Yes	Yes		Yes	ON	
CCERT participation	No	Yes	Yes	Yes	Yes	Ves	2 2	2 2
SE I participation	No	Yes	Yes	Yes	S	Vec	2 2	2 2
Have a department computer emergency resp. (DCERT)	No	Yes	Yes	Yes	S	Yes	2 2	2 2
Systems implemented and configured to security standards	, yes	Yes	Yes	Yes	Yes	Yes	νσΛ	200
Employees sign acceptable use agreement	Yes	Yes	Yes	Yes	Yes	Yes	20. 20.	SD /
Passwords changed every 90 days	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Prilysical security measures in place	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data samutzanon prior to disposal	Yes	Yes	∵,Yes	Yes	SeA	Yes	Yes	Yes
rorma security development lifecycle	No	Yes	Yes	Š	8	Yes	Voc	Z
Vulnerability assessment scanning performed	No	No	8	2	Yes	No	2	2 2
remote access to servers allowed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Vec.
I wo ractor authentication required for remote access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
nemote dial access allowed	ON.	No	No.	©N.	Yes	ON	eN	CZ
Demission of the specific remote access software	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Ves
nequire remote access via VPN	Yes	Yes	Yes	°N	Yes	Yes	Ype	Voc
Do you have obsolete computer operating systems	No	No	No	Yes	ON No	S ON		
Do you have a technology refresh plan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Vac
Do you rerquire firewalls on desktops and laptops	Yes	N/A	Yes	No	_S	2	2	2
HOST IIITUSION ON SERVERS	No	Yes	S N	No	2	S	Yes	2
is antivirus software installed and current	Yes	Yes	Yes	Yes	Yes	Ves	Yes	Yec
Is antivirus software centrally managed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	SO A
Is parch management software utilized	λes	Yes	Yes	Yes	Yes	Yes	Vec	Voe
Are security software patches current	Se X	Yes	Yes	Model	γes	Vac	2027	000
BCP Plan development started	Yes	Yes	Yes	Yes	Yes	Yes	Vac.	S A
Crisis Mgmt Plan	Yes	Yes	Yes	Yes	9	9	8.8	3 2

Departmental Security Rating

Color Codes
Good Security Program
Some Deficiencies
Major Weaknesses
Not Applicable



Question	Counsel	DA	Fire	DHG	H TO		<u> </u>	į
Compliant With Board security policies	Yes	Yes	Vac		Name need	בוק	ISAB	20
If not, do you have a compliance plan	NITA	0	601	3	res	Yes	Yes	Yes
Will volt he compliant in 2007/2000	IN/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Decimated compliant in confiction	N/A	N/A	N/A	A/A	N/A	NI/A	VIIV	N.I.A
Designated security officer	Part Time	Part Time	Part Time	Full Timo		U/21 C	3.	A/N
Attend ISSC regularly	S	Voc	2 22	DILLIO II		ranıme	Full lime	Full Time
CCERT participation	2 2	000	res	Yes	ON No	Yes	Š	Yes
SET participation	001	Yes	Yes	Yes	%	Yes	Yes	Yes
Have a denartment computer computer	0N	No	Yes	Yes	SN S	Yes	Yes	Vac
	S	No	Yes	sey	2	Yes	Yee	S 2
Employees sign security standards	Yes	Yes	Yes	Yes	Yes	Vec	Voc	2 2
December 5 sign acceptable use agreement	Yes	None	Yes	Yes	Vec	20 X	200	Les
rasswords changed every 90 days	Yes	Yes	Yes	Voc	3 8	001	SP .	Yes
Physical security measures in place	Voc	20.7	20.7	יתה	res	res	Yes	Yes
Data sanitization prior to disposal	5 5	CD -	res	Yes	Yes	Yes	Yes	Yes
Formal security development lifecycle	ST L	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Vulnerability assessment scanning noutering	2	8	No	Yes		Yes	Yes	Š
Remote access to servers allowed	2	8	No	Yes	SeX	Yes	cN	Voc
Two Factor authorations	No	Yes	Yes	Yes	Yes	Vec	Vac	200
Remote dial access	Yes	Yes	Yes	Yes	Yes	Yes	20. Vos	00A
House identified access allowed	Yes	oN	Yes	No	No	200	S N	100
Trave Identified Specific remote access software	l Kes	Yes	S	202	214	2	ON!	res
Require remote access via VPN	No.	200		รยา	ON .	Yes	Yes	No
Do you have obsolete computer operating exetage	S Z	ב ב	res	Yes	Yes	Yes	Yes	Yes
Do you have a technology refresh plan) S	ON ,	S S	No	 No	ON .	S S	Yes
Do you rerquire firewalls on desktons and lantons	Yes	Yes	Yes	Yes	Yes	Yes	Yes	S
Host intrusion on servers	0N	Yes	Yes	Yes	No	Yes	Yes	8
Is antivirus software installed and current	2	02	2	No	No	No	2	S
Is antivirus software centrally managed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Vac
Is natch management software utilized	Yes	Yes	Yes	Yes	Yes	Yes	Ves	Vec
Are contributed finance and the contributed	Yes	Yes	Yes	Yes	Yes	Ves	Voc	200
PCD Dies dereil	Yes	Yes	Yes	Yes	Vac	Voc	3 3	100
Dor Flail development started	Yes	Yes	Yes	Voc	20.7	50-	L GS	Yes
Crisis Mgmt Plan	Yes	Voc	3 2	3	OD .	res	Yes	Yes
		3		res	0N	2	ON N	Yes
Departmental Security Dating								

Departmental Security Rating

Color Codes
Good Security Program
Some Deficiencies
Major Weaknesses
Not Applicable



Question	HMQ	Mil & Vot	Ombilda	ָרָבְּיִר בְּיִבְּיִר בְּיִרְבְּיִר בְּיִרְבְּיִר בְּיִרְבְּיִרְבְּיִר בְּיִרְבְּיִרְבְּיִרְבְּיִרְבְּיִרְבְּי		-		
Compliant with Board security policies	Yes	Ype	Special Vol.	Lain hec	Frobat	Pubdet	Pub Hith	Library
If not, do you have a compliance plan	N//V	N 1/A	2D-	SAL	Yes	Yes	No	Yes
Will you be compliant in 2007/2008	¥/NI	N/A	N/A	N/A	Yes	N/A	Yes	N/A
Designated sociality office.	N/A	N/A	N/A	N/A	Yes	N/A	Vec	N/A
Attend 1960	Full Time	Part Time	Full Time	Part Time	Full Time	Full Time	Dart Timo	Dart Timo Eill Timo
Allelid ISSC regularly	Yes	No	Yes	å	Yes	Vec	Voc	
Coent participation	Yes	8	Yes	Z	So.	3	103	r do
SEI participation	Yes	S	Yac	Q Z	80-	00.7	res	Yes
Have a department computer emergency resp. (DCERT)	Vac	2 2	Vec	02/2	res	Yes	Yes	Yes
Systems implemented and configured to security standards	20/2	0N-	res	oN,	Yes	Yes	Yes	Yes
	65-	SEL	res	Yes	Yes	Yes	Yes	Yes
Passwords changed every 90 days	res	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Physical security measures in place	Sea	ON ;	Yes	Yes	No	Yes	Yes	Yes
Data sanitization prior to disposal	Yes	Yes	Yes	Yes	Хes	Yes	Yes	Yes
Formal security development lifewals	Yes	Yes	Yes	Yes	Yes	, Yes	Yes	Yes
Vilherability acceptant con :	8	Yes	Yes	oN	oN N	Yes	2	Z
Remote access to course of the control of the contr	Yes	Yes	No	Yes	2	S	Ves	2
Two Earlor authorations	Yes	No	No	Yes	Yes	Yes	Yes	S A
Remote dial access allowed	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Xex
Have identified enotific somethers	S.	No	ON	No	No	ş	Yes	
Recluire remote access via VDN	Yes	8	N/A	N/A	Yes	2	Yes	Yes
Do vou have obsolete computer constitution	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Do you have a technology refrash plan	oN,	oN.	<u>@</u>	No	No	Yes	S.	ON No
Do vou rerduire firewalls on desktons and lantage	X-es.	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Host intrusion on servers	2	Yes	Yes	Yes	. Yes	2	2	Yes
Is antivirus software installed and current	ON ;	Yes	Yes	Yes	No	8	2	Yes
Is antivirus software centrally managed	Se X	Yes	Yes	Yes	Yes	Yes	Kes	Yes
Is patch management software utilized	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Are security software natches current	Yes	Yes	Yes	Yes		Yes	Yes	Yes
BCP Plan development started	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Crisis Mamt Plan	Yes	Yes	Yes	Yes	Xex	Yes	Yes	Yes
	Kes	ON No	Yes	No	Yes	Yes	2	Yes

Departmental Security Rating

Color Codes
Good Security Program
Some Deficiencies
Wajor Weaknesses
Not Applicable



N/A N/A		Yes N/A N/A B Part Time Yes Yes		Yes N/A Full Time Yes Yes Yes Yes Yes Yes Yes	Yes Yes
N/A				N/A Full Time: Yes: Yes: Yes: Yes: Yes: Yes:	Yes
N/A N/A N/A Part Time Part Time Yes Yes No No No Yes No No No No No No No No				N/A Full Time Yes Yes Yes Yes	Yes Yes Yes Yes Yes Yes Yes Yes Yes
Part Time Part Time Ves Ves				Full Time Yes Yes Yes Yes Yes Yes	Full Time Yes Yes Xes Xes Yes Yes
Yes Yes Yes Yes Yes Yes rity standards Yes Yes Yes Yes<				Yes Yes Yes Yes Yes Yes	Yes Yes Yes Yes Yes Yes
Yes Yes		Yes Yes Yes Yes Yes Yes Yes	Yes Yes Yes No No	Yes.	Yes Yes Yes Yes
Ves Yes Yes		Yes Yes Yes Yes Yes Yes	Yes Yes Yes Yes Yes	Yes Yes Yes.	Yes Yes Yes
(DCERT) Yes Yes rity standards Yes Yes Yes Yes Yes No No No Yes Yes Yes		Yes Yes Yes Yes	Yes Yes No Yes	Yes	Yes Yes Yes
Pes Fes Fes Ves Yes Yes Ves Yes Yes Ves Ves Ves Ves		Yes	Yes Yes No Yes	Yes	Yes
rity standards Yes Yes Yes Yes Yes		Yes Yes Yes Yes	Yes No Yes	Yes.	Yes
Yes Yes No No Yes Yes		Se),	yes No Yes		
Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes No No Yes Yes		Yes Yes Yes	No Yes	Now	Yes
Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes No Yes No Yes Yes Yes		Yes	Yes	Yes	Yes
Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes No No No Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes		Yes		Yes	Yes
Yes Yes access Yes Yes no No No no Yes re No Yes res Yes		Vac	∠es	Yes	Yes
Yes Yes access Yes Yes No No No re No Yes Yes Yes Yes tems No No		3	Yes	2	S
Yes Yes remote access Yes Yes Software No Yes Yes Yes Yes ing systems No No		2	Yes	8	2
remote access Yes Yes No No No software No Yes Yes Yes ing systems		Yes	Yes	Yes	Yes
software No No No Yes Yes ing systems No No	5 10 10 11 11 11	Yes	Yes	Yes	Yes
software No Yes Yes Yes ing systems No No	7-1-1-1 1-1-1-1	. ON	No	Yes	Yes
Yes Yes ing systems No No	es Yes	S N	SN N	Yes	Yes
ing systems No No	se Yes	Yes	Yes	Yes	Yes
の一般の一般のでは、「ないのでは、「ないのでは、「ないのでは、「ないのでは、「ないのでは、「ないのでは、「ないのでは、」では、「ないのでは、」」」、「ないのでは、「ないのでは、「ないのでは、「ないのでは、「ないのでは、」」、「ないのでは、「ないのでは、「ないのでは、「ないのでは、」」、「ないのでは、「ないのでは、「ないのでは、」」、「ないのでは、「ないのでは、「ないのでは、」」、「ないのでは、「ないのでは、「ないのでは、」」、「ないのでは、「ないのでは、」」、「ないのでは、「ないのでは、」」、「ないのでは、「ないのでは、」」、「ないのでは、」」、「ないのでは、」」、「ないのでは、」」、「ないのでは、」」、「ないのでは、」」、「ないのでは、」」、「ないのでは、」」、「ないのでは、」」、「ないのでは、」」、「ないのでは、」」、「ないのでは、」」、「ないのでは、」」、「ないのでは、」」、「ないのでは、」」、「ないのでは、」」、「ないのでは、これでは、「ないのでは、これでは、これでは、これでは、これでは、これでは、これでは、これでは、これ		No	ON	oN N	Yes
	se Yes	Yes	Yes	Yes	Yes
Do you rerquire firewalls on desktops and laptops No		S N	SN.	Yes	Yes
Yes	oN o	Yes	Š	2	S N
nt Yes Yes	se Yes	Yes	Yes	Yes	Yes
Yes Yes	se Yes	yes.	Yes	Yes	Yes
Yes	ss Yes	Yes	Хes	Yes	Yes
current	se Yes	Yes	Хes	Yes	Yes
oment started Yes Yes		Yes	Yes	Yes	Yes
Crisis Mgmt Plan	se Ves	, Yes	9 N	S N	Yes

Color Codes Good Security Program Some Deficiencies Major Weaknesses Not Applicable

Departmental Security Rating

